IN THE UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF DELAWARE

SRI INTERNATIONAL INC., a California corporation,	)	
Plaintiff,	)	
v.	)	Civ. No. 04-1199-SLR
INTERNET SECURITY SYSTEMS, INC., a Georgia corporation, SYMANTEC CORPORATION, a Delaware corporation, and INTERNET SECURITY SYSTEMS, INC., a Delaware corporation,	)	
Defendants.	)	

Thomas L. Halkowski, Esquire, Timothy Devlin, Esquire, and Kyle Wagner Compton, Esquire of Fish & Richardson P.C., Wilmington, Delaware, Counsel for Plaintiff. Of Counsel: Frank E. Scherkenbach, Esquire of Fish & Richardson P.C., Boston, Massachusetts, Howard G. Pollack, Esquire and Katherine D. Prescott, Esquire of Fish & Richardson P.C., Redwood City, California, and Todd G. Miller, Esquire and Michael M. Rosen, Esquire of Fish & Richardson P.C., San Diego, California.

Richard L. Horwitz, Esquire and David E. Moore, Esquire of Potter Anderson & Corroon LLP, Wilmington, Delaware. Counsel for Defendants Internet Security Systems, Inc., a Delaware corporation and Internet Security Systems, Inc., a Georgia corporation. Of Counsel: Alison H. Alterson, Esquire and Scott T. Weingaertner, Esquire of King & Spalding, LLP, New York, New York; Adam M. Conrad, Esquire of King & Spalding, LLP, Charlotte, North Carolina; and Holmes J. Hawkins III, Esquire, Natasha H. Moffitt, Esquire and Charles A. Pannell III, Esquire of King & Spalding, LLP, Atlanta, Georgia.

Richard K. Hermann, Esquire and Mary Matterer, Esquire of Morris James LLP, Wilmington, Delaware. Counsel for Defendant Symantec Corporation. Of Counsel: Robert M. Galvin, Esquire, Paul S. Grewal, Esquire, Renee DuBord Brown, Esquire, Geoffrey M. Godfrey, Esquire and Katie J.L. Scott, Esquire of Howrey LLP, Cupertino, California.

MEMORANDUM OPINION

Dated: August 20, 2009
Wilmington, Delaware

ROBINSON, District Judge

I. INTRODUCTION

On August 26, 2004, plaintiff SRI International, Inc. ("SRI") brought suit against defendants Symantec Corporation ("Symantec") and Internet Security Systems, Inc. ("ISS") (collectively, "defendants") charging infringement of four patents: United States Patent Nos. 6,484,203 ("the '203 patent"), 6,708,212 ("the '212 patent"), 6,321,338 ("the '338 patent"), and 6,711,615 ("the '615 patent"). On April 13, 2005, the court denied defendants' motions to dismiss, sever and transfer. (D.I. 31) Following discovery, Symantec moved for summary judgment of non-infringement (D.I. 286), ISS moved for summary judgment of non-infringement and invalidity (D.I. 282, 291, 364), and defendants jointly moved for summary judgment that each of the patents in suit is invalid pursuant to 35 U.S.C. § 102 and § 103 (D.I. 297). Plaintiff filed motions for summary judgment of validity. (D.I. 270, 276, 279) The court issued its claim construction opinion on October 17, 2006. (D.I. 468) On the same date, the court held each of the asserted patents invalid as anticipated by SRI's prior art publication "Live Traffic Analysis of TCP/IP Gateways" ("Live Traffic") pursuant to 35 U.S.C. § 102. The court also found the '212 patent invalid as anticipated by a paper entitled "EMERALD: Event Monitoring Enabling Responses To Anomalous Live Disturbances" ("EMERALD 1997") pursuant to 35 U.S.C. § 102. (D.I. 471[1]) On appeal, the Federal Circuit affirmed the court's decision with respect to the '212 patent and vacated and remanded the court's determination that the remaining patents were rendered invalid by Live Traffic. *SRI Int'l, Inc. v. Internet Sec. Sys., Inc.*, 511 F.3d 1186 (Fed. Cir. 2008). The court

---

[1]*SRI Int'l, Inc. v. Internet Sec. Sys., Inc.*, 456 F. Supp. 2d 623 (D. Del. 2006).

denied defendants' renewed motion for summary judgment of invalidity (D.I. 297) on August 21, 2008. (D.I. 525)

A jury trial commenced September 2, 2008. Plaintiff asserted that defendants infringe claims 1 and 12 of the '203 patent and claims 1, 13, 14, and 16 of the '615 patent. Plaintiff asserted that ISS also infringes claims 1, 11, 12, 13 and 24 of the '338 patent. Defendants challenged the validity of the asserted patents. On September 18, 2008, the jury found that Symantec and ISS infringed each asserted claim of the '615 and '203 patents, that ISS did not infringe the '338 patent, and that each of the '203, '605 and '338 patents are valid. (D.I. 558) The parties filed their post-trial motions on October 14, 2008. Currently pending before the court are: (1) plaintiff's motion for post-trial relief (D.I. 564); (2) ISS's motion for renewed judgment as a matter of law ("JMOL") or, in the alternative, for a new trial (D.I. 565); (3) Symantec's motion for a new trial and/or to alter or amend the judgment (D.I. 566); and (4) Symantec's motion for JMOL (D.I. 567).

II. BACKGROUND

A. Patents in Suit

The patents in suit relate to the monitoring and surveillance of computer networks for intrusion detection. In particular, the patents teach a computer-automated method of hierarchical event monitoring and analysis within an enterprise network that allows for real-time detection of intruders. Upon detecting any suspicious activity, the network monitors generate reports of such activity. The claims of the '203 and '615 patents focus on methods and systems for deploying a hierarchy of network monitors

that can generate and receive reports of suspicious network activity.

To detect attacks which do not possess deterministic signatures or to detect previously unknown (new) attacks, the patents in suit disclose the use of statistical detection methods on network data. The claims of the '338 patent are directed to a particular statistical algorithm for detecting suspicious network activity.

The patents in suit share a common specification and priority date of November 9, 1998. The critical date is November 9, 1997 for purposes of 35 U.S.C. § 102(b).

1. The '615 and '203 patents

Plaintiff asserted that defendants infringe claims 1, 13, 14 and 16 of the '615 patent and claims 1 and 12 of the '203 patent. Independent claims 1 and 13 of the '615 patent read as follows:

> 1. A computer-automated method of hierarchical event monitoring and analysis within an enterprise network comprising: deploying a plurality of network monitors in the enterprise network; detecting, by the network monitors, suspicious network activity based on analysis of network traffic data selected from one or more of the following categories: {network packet data transfer commands, network packet data transfer errors, network packet data volume, network connection requests, network connection denials, error codes included in a network packet, network connection acknowledgements, and network packets indicative of well-known network-service protocols}; generating, by the monitors, reports of said suspicious activity; and automatically receiving and integrating the reports of suspicious activity, by one or more hierarchical monitors.
>
> 13. An enterprise network monitoring system comprising: a plurality of network monitors deployed within an enterprise network, said plurality of network monitors detecting suspicious network activity based on analysis of network traffic data selected from one or more of the following categories: {network packet data transfer commands, network packet data transfer errors, network packet data volume, network connection requests, network connection denials, error codes included in a network packet, network connection acknowledgements, and network packets indicative of well-known network-service protocols}; said network monitors generating reports of said suspicious activity; and one or more hierarchical monitors in the enterprise

network, the hierarchical monitors adapted to automatically receive and integrate the reports of suspicious activity.

As used in all of the claims in suit, a "network" is a "collection of software and/or hardware interconnected by communication links for sharing information." (D.I. 468 at 2) A "packet" is a "group of data bytes which represents a specific information unit with a known beginning and end." (*Id.*) "Network monitors" means "[s]oftware and/or hardware that can collect, analyze and/or respond to data." (*Id.*)

Asserted claims 14 and 16 are dependant on claim 13, adding the additional limitations that the "integration comprises correlating intrusion reports reflecting underlying commonalities" (claim 14) and that the "plurality of network monitors include an application programming interface (API) for encapsulation of monitor functions and integration of third party tools" (claim 16).

Claims 1 and 12 of the '203 patent are independent claims and claim similar subject matter to that of the '615 patent, with the exception that the '203 patent claims do not require "network connection acknowledgments" or "network packets indicative of well-known network-service protocols" (as in claim 13 of the '615 patent). Claims 1 and 12 read as follows:

> 1. A computer-automated method of hierarchical event monitoring and analysis within an enterprise network comprising: deploying a plurality of network monitors in the enterprise network; detecting, by the network monitors, suspicious network activity based on analysis of network traffic data selected from the following categories: {network packet data transfer commands, network packet data transfer errors, network packet data volume, network connection requests, network connection denials, error codes included in a network packet}; generating, by the monitors, reports of said suspicious activity; and automatically receiving and integrating the reports of suspicious activity, by one or more hierarchical monitors.
>
> 12. An enterprise network monitoring system comprising: a plurality of network

monitors deployed within an enterprise network, said plurality of network monitors detecting suspicious network activity based on analysis of network traffic data selected from the following categories: {network packet data transfer commands, network packet data transfer errors, network packet data volume, network connection requests, network connection denials, error codes included in a network packet}; said network monitors generating reports of said suspicious activity; and one or more hierarchical monitors in the enterprise network, the hierarchical monitors adapted to automatically receive and integrate the reports of suspicious activity.

2. The '338 patent

The '338 patent relates to using a statistical method to detect suspicious network activity. Plaintiff asserted that ISS infringes claims 1, 11, 12, 13 and 24 of the '338 patent. Independent claim 1 reads as follows:

1. A method of network surveillance, comprising:
receiving network packets handled by a network entity;
building at least one long-term and at least one short-term statistical profile from at least one measure of the network packets, the at least one measure monitoring data transfers, errors, or network connections;
comparing at least one long-term and at least one short-term statistical profile; and determining whether the difference between the short-term statistical profile and the long-term statistical profile indicates suspicious network activity.

The court construed "building at least one long-term and at least one short-term statistical profile from at least one measure of the network packets" to mean:

Generating at least two separate data structures, one a statistical description representative of historical network activity, and one a statistical description of recent network activity, where the statistical descriptions are based on at least one measure of the network packets and are generated through the use of statistical analysis; *i.e.*, something more than simply collecting and receiving data.

(D.I. 468 at 5) The phrase "determining whether the difference between the short-term statistical profile and the long-term statistical profile indicates suspicious network activity" was construed to mean "[u]sing the result of the comparison to decide whether the monitored activity is suspicious." (*Id.* at 6)

Claim 11 depends from claim 1 and adds the additional limitations of "responding based on the determining whether the difference between the short-term statistical profile and the long-term statistical profile indicates suspicious activity." "Responding" was defined as "[t]aking an action in response, including both passive and active response." (*Id.* at 5) Claim 12 depends further from claim 11, adding the requirement that "responding comprises transmitting an event record to a network monitor."

Claim 13 depends further from claim 12, and requires "transmitting the event record to a hierarchically higher network monitor." A "hierarchically higher network monitor" was construed to mean "[a] network monitor that receives data from at least one network monitor that is at a lower level in the analysis hierchy." (*Id.* at 3)

Independent claim 24 is similar to claim 1, but is written in the form of a product claim, as follows:

> 24. A computer program product, disposed on a computer readable medium, the product including instructions for causing a processor to:
> receive network packets handled by a network entity;
> build at least one long-term and at least one short-term statistical profile from at least one measure of the network packets, the measure monitoring data transfers, errors, or network connections;
> compare at least one short-term and at least one long-term statistical profile; and
> determine whether the difference between the short-term statistical profile and the long-term statistical profile indicates suspicious network activity.

B. Accused Products

1. Symantec

Plaintiff asserted that a specific combination of Symantec products infringes the '203 and '615 patents: Symantec Gateway Security 5400, 5600 and 1600 Series (the "SGS Products") **in combination with** the Incident Manager 3.0 or the Security

Information Manager Series 9500 appliances (the "Manager Products"). The SGS Products are lower-level network monitors and the Manager Products are hierarchical network monitors. Symantec does not dispute that, where a Manager Product is deployed with two or more SGS Products in an enterprise network, and the Manager Product is configured to automatically receive and integrate reports of suspicious network activity generated by the SGS Products, the '615 and '203 patents are infringed. (D.I. 572 at 7)

Plaintiff also accused Symantec's iForce IDS, ManHunt 3.0, Symantec Network Security 4.0, and the Symantec Network Security 7100 Series appliances (the "ManHunt" products) of infringement. The ManHunt products are not the subject of any post-trial motions.

2. ISS

Plaintiff accused the following ISS products of infringing the '203 and '615 patents: RealSecure Network, Guard, Server, and Desktop series and Proventia A, G, M, Server, and Desktop series (the "ISS Sensors") in combination with Fusion 2.0. The ISS accused products for the '338 patent are the Proventia Anomaly Detection System products (hereinafter, "ADS").

ADS, through its "rate-based anomaly detection" feature, "[d]etects sudden shifts from baselined traffic levels over time." (PTX-106 at 3) This is accomplished by determining the current traffic rate, or the traffic rate in bits per second based on an observation of traffic over a two-minute time period. ADS also determines an historic traffic rate by using average traffic rate information from longer periods of time, such as a day, week, or month. The current and historic traffic rates are compared; if the

current rate exceeds the historical rate, an alert is generated. (D.I. 592 at 496:2-498:6; 501:9-21; D.I. 604 at 1743:8-1744:5) The alert is forwarded to the "SiteProtector" product, a management system for ISS products. (D.I. 593 at 502:1-4; 639:1-6; PTX-106 at 2) "SiteProtector" is the general name for ISS's management software, or software that receives and integrates reports of suspicious activity received from an ISS Sensor. Version 2.0 of ISS's "SiteProtector Security Fusion" product, or "Fusion 2.0," is an add-on software module.

C. Asserted Prior Art

1. The JiNao Report

At trial, ISS argued that the '338 patent is anticipated by a "Technical Report" entitled "Architecture Design of a Scalable Intrusion Detection System for the Emerging Network Infrastructure" by Frank R. Jou et al. ("the JiNao Report"). (DTX-51) The JiNao Report describes the architecture of an intrusion detection system that protects against attacks on network infrastructure, such as routers. To do so, the system described monitoring router activity, using statistical profiling on router audit logs. The parties disputed at trial whether the JiNao Report disclosed building statistical profiles based on network packet data as required by the patents in suit.

2. Live Traffic

The Live Traffic paper was discussed in the court's prior opinion, *SRI Intern., Inc.*, 456 F. Supp. 2d at 626. In short, the Live Traffic paper was submitted by Phillip Porras ("Porras"), one of the named inventors of the patents in suit, to the Internet Society in 1997 in response to a call for papers for a conference called the "Symposium

on Network and Distributed System Security" ("SNDSS"). Matt Bishop ("Bishop") was the program chair for the SNDSS who received Porras's submission by email dated August 1, 1997. In addition, Porras provided a link to plaintiff's FTP[2] site whereon a copy of the Live Traffic paper was posted for one week. The Live Traffic paper was authored by Porras and Alfonso Valdes ("Valdes"), another named inventor of the patents in suit, and it is undisputed that, if the Live Traffic paper is 35 U.S.C. § 102(b) prior art, it anticipates each patent in suit.

3. RealSecure

RealSecure is a ISS software product responsible for alerting a user when an unauthorized individual breaks into an enterprise network. There are two components of the product: a sensor and a console (or user interface). (D.I. 593 at 763:3-13)

> The RealSecure management console displays real-time alarm data in a standard Windows NT activity tree mode, where the data in the tree can be sorted by destination address, source address, or event name. Events contain an icon that indicates the severity as well as a distinct event name. Multiple occurrences of the same event are combined into a single notification. The user can drill down into event data to find out exactly what happened, what actions RealSecure took in response to the event, and what other related events have also occurred. Event data can also be stored in an ODBC-compliant database for generalization of reports. Reports are available in text and graphic formats and the user can launch customized reports from the interface, if desired.

(DTX-1801 at 3496; D.I. 594 at 819:4-820:19[3]) There are several ways to view the

---

[2]FTP, or file transfer protocol, is a protocol for exchanging files over any computer network that supports the TCP/IP protocol (such as the Internet or an intranet). Plaintiff maintained a FTP server.

[3]ISS's witness confirmed the validity of this summary for how RealSecure worked in the 1996-1997 timeframe. The testimony indicated that several versions of RealSecure were released before 1997, and several more between 1997 and 2000. (D.I. 593 at 760:25-761:1; DTX-879) The parties do not call out specific differences between the versions in their post-trial papers.

activity tree window. One is the "source tab," where network activity is sorted by the source of the system initiating the activity. (DTX-2542 at 62) The name is followed by a numerical value corresponding to the number of events for that source, *e.g.*, "duke (2)." (*Id.*) This same format is used for the "events tab," where "the most recent network activity [is] sorted by the type and priority of the event." (*Id.* at 64) Finally, an alternate view is the "destination tab," which sorts events by the numerical IP addresses of the systems targeted by the activity. (*Id.* at 63) Aside from reporting events to the console for the user's viewing in these manners, the RealSecure system can take other responsive measures, such as sending emails, killing the connection, and stopping network traffic. (D.I. 593 at 759:10-24) The parties disputed at trial whether RealSecure integrated reports of suspicious activity as required by the hierarchical monitor claim limitation.

4. DIDS 1991

In 1991, Steven R. Snapp et al. of the University of California, Davis published a paper entitled "DIDS (Distributed Intrusion Detection System) – Motivation, Architecture, and An Early Prototype" (hereinafter, the "DIDS 1991 paper"). (DTX-21) The DIDS 1991 paper described the DIDS Project, a multi-organizational intrusion detection project that was developed in 1990 and funded through the United States Air Force. (D.I. 594 at 999:22-1002:6) The components of the prototype DIDS intrusion detection system described by the DIDS 1991 paper "include[d] the DIDS director, a single host monitor per host, and a single LAN[4] monitor for each LAN segment of the monitored

[4]Local area network. Generally, a network covering a small physical area, as compared to a wide area network.

network." (DTX-21 at 168) In Figure 2, the DIDS 1991 paper depicts a single "LAN Monitor" connected to a "DIDS Director" containing the user interface. (*Id.* at 176) The DIDS 1991 paper also describes that the "LAN monitor uses several simple analysis techniques to identify significant events," such as profiles of expected network behavior. (*Id.* at 171)

The parties do not dispute that the DIDS 1991 paper is 35 U.S.C. § 102(b) prior art. The dispute at trial focused on whether the DIDS 1991 paper disclosed and enabled multiple lower level (or LAN) monitors as required by the "plurality of network monitors in the enterprise network" limitation.

5. EMERALD 1997

EMERALD 1997 was also discussed in the court's prior opinion, *SRI Intern., Inc.*, 456 F. Supp. 2d at 626, and by the Federal Circuit, *SRI Intern., Inc.*, 511 F.3d at 1188-89. In short, EMERALD 1997 is a conceptual overview of the EMERALD system, the brainchild of plaintiff's EMERALD project on intrusion detection, published by Porras and Peter G. Neumann on behalf of plaintiff in October 1997. EMERALD 1997 contains a detailed description of plaintiff's early research in Intrusion Detection Expert System ("IDES") technology, and outlines the development of the Next Generation IDES ("NIDES") for detecting network anomalies.

The parties do not dispute that EMERALD 1997 is 35 U.S.C. § 102(b) prior art to the patents in suit. With respect to anticipation, the parties dispute only whether EMERALD 1997 discloses detection of any of the network traffic data categories listed in claim 1 of the '203 and '615 patents. With respect to obviousness, the parties

dispute whether EMERALD 1997's internal citation to a publication entitled "A Method to Detect Intrusive Activity in a Networked Environment" (hereinafter, "Intrusive Activity 1991"), one of twenty-four citations to outside references contained in that paper, provides a motivation to combine the references and a reasonable expectation of success with respect to the inventions claimed in the '203 and '615 patents. It is not disputed that Intrusive Activity 1991 discloses at least one of the claimed categories of network traffic data.

D. The Verdict

With respect to Symantec, the jury found that both the ManHunt Products and the asserted combination of SGS Products with the Manager Products infringe each asserted claim of the '203 and '615 patents.[5] (D.I. 558) The jury also found that Symantec induces the infringement of each asserted claim by its customers. (*Id.*)

The jury found that ISS infringes each asserted claim of the '203 and '615 patents and that ISS induces infringement by its customers of each of these claims. (*Id.*) The jury also found that ISS does not infringe the '338 patent. (*Id.*) Finally, the jury found that defendants did not prove that the patents in suit are invalid due to anticipation, or that the '203 or '615 patents are invalid due to obviousness or failure to disclose the best mode.[6] (*Id.*) The court entered judgment for plaintiff on the '203 and '615 patents and for ISS on the '338 patent. (D.I. 560)

---

[5]Symantec does not address the portion of the verdict regarding Manhunt Products in its post-trial brief. (D.I. 572)

[6]Defendants do not challenge the verdict with respect to best mode in their post-trial papers.

IV. DISCUSSION

A. Infringement

1. Standards

A patent is infringed when a person "without authority makes, uses or sells any patented invention, within the United States . . . during the term of the patent." 35 U.S.C. § 271(a). A two-step analysis is employed in making an infringement determination. *Markman v. Westview Instruments, Inc.*, 52 F.3d 967, 976 (Fed. Cir. 1995). First, the court must construe the asserted claims to ascertain their meaning and scope. *Id.* Construction of the claims is a question of law subject to de novo review. *See Cybor Corp. v. FAS Techs.*, 138 F.3d 1448, 1454 (Fed. Cir. 1998). The trier of fact must then compare the properly construed claims with the accused infringing product. *Markman*, 52 F.3d at 976. This second step is a question of fact. *See Bai v. L & L Wings, Inc.*, 160 F.3d 1350, 1353 (Fed. Cir. 1998).

"Direct infringement requires a party to perform each and every step or element of a claimed method or product." *BMC Res., Inc. v. Paymentech, L.P.*, 498 F.3d 1373, 1378 (Fed. Cir. 2007). "If any claim limitation is absent from the accused device, there is no literal infringement as a matter of law." *Bayer AG v. Elan Pharm. Research Corp.*, 212 F.3d 1241, 1247 (Fed. Cir. 2000). If an accused product does not infringe an independent claim, it also does not infringe any claim depending thereon. *Wahpeton Canvas Co. v. Frontier, Inc.*, 870 F.2d 1546, 1553 (Fed. Cir. 1989). The patent owner has the burden of proving infringement and must meet its burden by a preponderance of the evidence. *SmithKline Diagnostics, Inc. v. Helena Lab. Corp.*, 859 F.2d 878, 889

(Fed. Cir. 1988) (citations omitted).

To demonstrate inducement of infringement, the patentee must establish "first that there has been direct infringement, and second that the alleged infringer knowingly induced infringement and possessed specific intent to encourage another's infringement." *Broadcom Corp. v. Qualcomm Inc.*, 543 F.3d 683, 697-98 (Fed. Cir. 2008) (citations omitted). That is, "inducement requires evidence of culpable conduct, directed to encouraging another's infringement, not merely that the inducer had knowledge of the direct infringer's activities." *DSU Medical Corp. v. JMS Co., Ltd.*, 471 F.3d 1293, 1306 (Fed. Cir. 2006) (citation omitted). "The plaintiff has the burden of showing that the alleged infringer's actions induced infringing acts and that he knew or should have known his actions would induce actual infringements." *Id.* (quoting *Manville Sales Corp. v. Paramount Sys., Inc.*, 917 F.2d 544, 553 (Fed. Cir. 1990)). This amounts to a showing of "specific intent." *Id.* at 1305 (citing *Warner-Lambert Co. v. Apotex Corp.*, 316 F.3d 1348, 1363 (Fed. Cir. 2003) and *Water Techs. Corp. v. Calco, Ltd.*, 850 F.2d 660, 668 (Fed. Cir. 1988) (patentee must prove that defendant "actively and knowingly aid[ed] and abett[ed] another's direct infringement")).

2. Symantec's motion for JMOL

Symantec moves for JMOL that the jury's verdict on induced infringement was not supported by substantial evidence because plaintiff presented no direct evidence that either Symantec or its customers actually employed the infringing combination of SGS and Manager Products. At trial, only a specific configuration of SGS and Manager Products was accused of infringement: the operation of the SGS and Manager

Products together in an enterprise network, where the Manager Product is configured to automatically receive and integrate reports of suspicious network activity generated by the SGS Products. There is no dispute that the SGS Products and Manager Products (independently) have non-infringing uses, or that the use of the products together in another configuration does not infringe.

Plaintiff built its infringement case upon an implication that Symantec's customers committed direct infringement. More specifically, plaintiff presented evidence that: (1) the SGS and Manager Products were designed to work together; (2) SGS Products are used to monitor enterprise networks; and (3) Symantec encouraged customers to employ both products together and provided instructions to customers on how to do so.

Plaintiff's evidence in this regard was as follows. A presentation with a "Costco" logo on its cover page, entitled "Symantec Incident Manager Overview," states that "Symantec Incident Manager is built upon SESA [Symantec Enterprise Security Architecture]" (PTX-33 at 0286105) and visually depicts the Symantec Enterprise Security Architecture as including "Incident Manager" for "correlation, analysis, and reporting" (*id.* at 0286128). Symantec product manager Howard Lev and engineer Paul Agbabian testified that the SGS and Manager Products work together. (D.I. 593 at 538:12-539:7, 543:6-18 (Symantec Incident Manager and Symantec Gateway Security Advance Manager can receive events from the SGS Products); 548:11-550:9, 551:12-15 (Symantec Incident Manager can receive information from at least the SGS 5400 series product and SNS 4.0 software))

Plaintiff's expert, Dr. George Kesidis ("Kesidis"), also testified that the SGS and

Manager Products are "design[ed] to operate with each other" and that SGS Products are used to monitor enterprise networks. (D.I. 593 at 626:4-15; 628:14-16; 743:13-15) Kesidis testified that, when customers buy the SGS and Manager Products, they receive manuals describing how they interoperate and, thus, it is reasonable to believe the customers will use the products together. (*Id.* at 626:4-15) Examples of materials provided to customers are: (1) the "Costco"-labeled materials noted previously (PTX-33; D.I. 593 at 629:1-23 (stating that his review of Symantec deposition testimony and other documents confirmed that the SGS Products send events to the Incident Manager, as depicted in PTX-33)); (2) a document entitled "Symantec Response for JPMorganChase Security Information and Event Management R[equest] F[or] I[nformation]" describing the use of Information Manager with network intrusion products (PTX-34 at 0286666-67 and -6678); and (3) a presentation entitled "Symantec Security Information Manager 9500 Series" containing a diagram connecting Information Manager with intrusion devices (PTX-167 at 0283912; D.I. 593 at 631:1-8 (Kesidis)).

Based upon this circumstantial evidence, plaintiff asserts that it was "well within the jury's province to conclude that, consistent with Symantec's encouragement and instructions, these products, which were designed to be used together in an enterprise network, were in fact used together." (D.I. 579 at 7) According to plaintiff, this would include infringement by Symantec itself ("undoubtably a large enterprise") by using its products in-house, and infringement by customers purchasing the SGS and Manager Products. (D.I. 579 at 3-4, 6-7) The court disagrees.

While it is true that circumstantial evidence may be used to demonstrate direct

infringement, *Moleculon Research Corp. v. CBS, Inc.*, 793 F.2d 1261, 1272 (Fed. Cir. 1986), the evidence must still indicate that infringement actually occurred. That is, a patentee must "either point to specific instances of direct infringement or show that the accused device necessarily infringes the patent in suit." *ACCO Brands v. ABA Locks Manufacturer Co., Ltd.*, 501 F.3d 1307, 1313 (Fed. Cir. 2007); *see also Dynacore Holdings Corp. v. U.S. Philips Corp.*, 363 F.3d 1263, 1275-76 (Fed. Cir. 2004).

In *ACCO*, the product accused of infringement (a key lock) could be operated in either an infringing manner or a non-infringing manner. *Id.* at 1310-11. The distributor's instructions provided with the product instructed customers to use the lock in the non-infringing manner.[7] *Id.* Plaintiff's expert opined at trial that the infringing method was the "natural and intuitive way to employ the device." *Id.* The record was, however, "devoid of evidence of actual users having operated the lock in an infringing manner," such as witness testimony or customer surveys. *Id.* at 1313. Stating that "[h]ypothetical instances of direct infringement are insufficient to establish vicarious liability or indirect infringement," the Federal Circuit found that the jury's verdict of inducement could not stand. *Id.* at 1313-14 (citation omitted). Therefore, where the claim language specifies a particular configuration, as compared to being "drawn to capability," the fact that an accused product (or combination of products) are "reasonably capable of being put into the claimed configuration is insufficient for a

---

[7]The manufacturer's instruction set included with the key lock described the infringing method, which required the use of a "hang card" not provided by the distributor. 501 F.3d at 1312. It appears that the manufacturer's instructions were not provided to the distributor's customers; the distributor substituted its own instructions for the accused product describing only the non-infringing method of use.

finding of infringement." *See Ball Aerosol and Specialty Container, Inc. v. Limited Brands, Inc.*, 555 F.3d 984, 994-95 (Fed. Cir. 2009) (citing *ACCO*, 501 F.3d at 1313). *Compare Intel Corp. v. U.S. Int'l Trade Comm'n*, 946 F.2d 821, 832 (Fed. Cir. 1991) (limitation of "programm**able** selection means" may be met by an accused device "capable of operating in the page mode," regardless of actual usage in that mode) (emphasis added) (cited by plaintiff).

In the case at bar, there is no dispute that the SGS and Manager Products, even where deployed in the same network, can be used together in a non-infringing manner. Symantec is correct that, because both the SGS and Manager Products have non-infringing uses (*i.e.*, the combination does not "necessarily infringe" the patents), plaintiff was obligated to identify specific instances of direct infringement involving these products.[8] *See ACCO,* 501 F.3d at 1313. In response to Symantec's motion, however, plaintiff failed to identify any evidence adduced at trial that either Symantec or any of its customers **actually** combined the SGS and Manager Products in an enterprise network where the Manager Products were also configured to automatically receive and integrate reports of suspicious network activity generated by the SGS Products.

The court recognizes that the Federal Circuit has previously found circumstantial evidence of direct infringement sufficient under more compelling circumstances. For example, in *Golden Blount, Inc. v. Robert H. Peterson Co.*, 438 F.3d 1354 (Fed. Cir.

---

[8]The court's instructions to the jury provided that "SRI must prove that the customer performed each and every step of a claimed method or made or used a product that satisfied each and every limitation of an asserted claim. If the customer omitted a single step or limitation recited in a claim, then you must find that the customer did not directly infringe that claim."

2006), the Court found that the district court did not err in concluding that defendant infringed the patent at issue, which claimed a fireplace assembly comprising a primary and secondary burner. In that case, the secondary burner sold by defendant had no non-infringing use, and defendant "provided [instruction sheets] to its customers on how to configure the components" resulting in the infringing combination. *Id.* at 1361. There was also no dispute that each end user who purchased a secondary burner attached it to a primary burner. *Id.* at 1326. The Federal Circuit stated that "it matters not that the assembled device can be manipulated into a non-infringing configuration, because the instructions packaged with each device teach the infringing configuration and nothing in the record suggests that either [defendant] or any end user ignored the instructions or assembled the burners in a manner contrary to the instructions so as to form a non-infringing configuration." *Id.* at 1363 (citation omitted).

In *Symantec Corporation v. Computer Associates International, Inc.*, 522 F.3d 1279 (Fed. Cir. 2008), the Federal Circuit addressed the issue on review of the district court's grant of summary judgment of non-infringement. Symantec, like plaintiff at bar, adduced only circumstantial evidence of direct infringement in opposition to defendant's motion. Symantec demonstrated, however, that defendant encouraged customers to use the accused product in an infringing manner. Notably, *Symantec* "[was] not a case where the customers may [have] be[en] using the product in an infringing way or a non-infringing way; [defendant's] customers c[ould] only use the [accused] products in an infringing way." *Id.* at 1293. Under those circumstances, the Federal Circuit reversed the grant of summary judgment by the district court notwithstanding Symantec's lack of

direct infringement evidence. *Id.*

In the present case, unlike in *Golden Blount*, the documents cited by plaintiff do not contain clear or affirmative instructions to employ the SGS and Manager Products together in an enterprise network, such that the Manager Products are configured to automatically receive and integrate reports of suspicious network activity generated by the SGS Products. The documents (even as characterized by plaintiff) simply depict the use of the SGS and Manager Products together. (PTX-33; PTX-34; PTX-167[9]) As in *ACCO*, plaintiff at bar did not present any witness testimony of defendant's employees or its actual customers demonstrating that direct infringement occurred.[10] Unlike *Symantec*, there was no dispute in this case that the SGS and Manager Products have non-infringing uses; it is only the specific configuration of the two together that was accused of infringement. Because plaintiff at bar presented no direct evidence of infringement and relied only on circumstantial evidence, the nature of which does not compel the conclusion that infringement necessarily occurred, the court finds

---

[9]Plaintiff does not discuss these documents in detail, notwithstanding, plaintiff does not point to any affirmative directions in these exhibits to employ the products together.

[10]Even a single infringing act may support a verdict of infringement. Plaintiff apparently sought to cast its theory of vicarious liability broadly, identifying a category of infringers (Symantec's customers buying both products) in order to seek a wider spectrum of damages. *See gen. Dynacore*, 363 F.3d at 1274 (citation omitted). Nevertheless, if Symantec's documents encouraged its customers to infringe, it follows that infringement would not be an isolated incident, and plaintiff should have been able to adduce evidence of at least one example of actual infringement. *See gen. Lucent Techs., Inc. v. Gateway, Inc.*, 543 F.3d 710, 723 (Fed. Cir. 2008) (finding no error in court's analysis that if using the infringing combination of software was "so common and so routine, then certainly [plaintiff] could have produced evidence of at least one instance" where infringement occurred). This observation also applies to plaintiff's case against ISS, discussed *infra*.

the jury's verdict of infringement of the '203 and '615 patents by the asserted combination of the SGS and Manager Products was not supported by substantial evidence.[11] Symantec's motion is granted. Because Symantec did not challenge the jury's finding that its ManHunt Products infringe the '203 and '615 patents, the court affirms the judgment for plaintiff in this regard.

3. Plaintiff's motion for JMOL

Plaintiff moves for JMOL that the jury's verdict that ISS does not infringe claims 1, 11, 12, 13 and 24 of the '338 patent is not supported by substantial evidence. Plaintiff accused ISS's ADS of infringing the '338 patent, which claims are generally directed to building and comparing long-term and short-term statistical profiles in order to determine suspicious network activity. The parties debated whether the current traffic rate generated by the ADS met the "short-term statistical profile" limitation of the claims. As noted previously, the court's construction required the "statistical descriptions" of both historical and current activity to be "based on at least one measure of the network packets and are generated through the use of statistical analysis; *i.e.*, something more than simply collecting and receiving data." (D.I. 468 at 5) The ADS creates a current traffic rate, or a measurement of the number of packets per unit of time, based upon a two-minute interval.

The parties characterized the current traffic rate as a "bit rate." The dispute at trial centered around whether this measurement is "statistical" in nature. Kesidis testified for plaintiff that the bit rate is a mathematical "average," and is a statistical

[11]The court need not address Symantec's specific intent to induce infringement.

measurement that satisfies the claims. (D.I. 593 at 674:10-11; 710:23-711:5; 713:18-25) ISS's expert, Dr. Steve Smaha ("Smaha"), testified that the current traffic rate is not an "average." According to Smaha, the current traffic rate is a count of the total amount of bytes that have been seen during the last two minutes, "convert[ed] into a rate by taking [this] total number of bits and dividing it by 120. That's not an average in any sense. It's just a bit rate over that period. We're not dividing it by the number of packets that we're seeing[.]" (D.I. 604 at 1743:15-20) Smaha used a demonstrative comparing the "simple math" of averages ("average of *N* terms = Sum of *N* items / *N*") to the "bit rate" ("Bit rate: # bits moved/Length of time"). (DTX-2203)

Smaha further testified that a "statistical description" requires both an average and a variance of the data. Smaha utilized a trial demonstrative showing that an "average" refers only to the center of a bell-shaped curve. The variance, or the width of that curve, would be required to have a statistical description of a particular curve. (D.I. 604 at 1744:13-25; DTX-2203) Smaha stated that the ADS does not look at "a select measure of data transfer, like the bits, find its mean [average], its variance, and create a statistical profile for it in the short-term." (D.I. 604 at 1746:11-21) In his opinion, ADS does not infringe because "all [it's] doing is measuring the bit rate during a two-minute window and there's definitely no mathematics that's more involved than computing the bit rate." (*Id.* at 1747:7-10) Similarly, Dr. Stuart Staniford, a scientist involved in the field of intrusion detection, testified that both a "measure" (of what is to be monitored) and a "profile" (which must be designed to "capture the odds of you going outside some range" of activity) are present in a statistical algorithm. (D.I. 594 at 862:7-868:24)

ISS points out that Kesidis agreed on cross-examination that "[s]tatistical

analysis has to deal with variations in data, variations in features and decisions under uncertainty[.]" (D.I. 593 at 710:16-25) Kesidis described a short-term statistical profile as follows:

> Well, it's short. There's a term to it, two minutes, and over that two-minute window, you could look at a select measure of data transfer, find its mean, **its variance**, create a statistical profile for it in the short-term.

(*Id.* at 675:3-6) (emphasis added) Kesidis agreed that standard deviation, representing the square root of the variance, is the "most fundamental" variation in a statistical measurement. (*Id.* at 711:6-11) Kesidis conceded that the ADS product does not store any variance; it does not "look[ ] at variability over the short-term." (*Id.*)

Plaintiff argues that the "rate" discussed by Smaha is not a "mere collection and reiteration of data" because the observed bits taken from the two-minute snapshot, after collection, are divided by the number of seconds it took to observe the bits. (D.I. 569 at 10) This division renders the result "a calculated figure obtained by applying mathematical analysis." (*Id.*) Smaha did not dispute that the bit rate was the result of simple mathematics, but stated that a "statistical profile" requires at least a mean, variance, or standard deviation, none of which are not calculated by ADS. (D.I. 604 at 1747:2-10)

The court finds that substantial evidence supports the jury's verdict of noninfringement. The jury could properly accept Smaha's testimony (over Kesidis's) and find that the bit rate is not an "average," and/or that the simple division resulting in the bit rate (or current traffic rate) is not "statistical" in nature because no variance or standard deviation is calculated. Finally, and contrary to plaintiff's assertion, ISS's

stipulation that a historical traffic rate is a long-term statistical profile is not necessarily inconsistent with its position regarding the short-term statistical profile. (D.I. 569 at 11) Plaintiff's witnesses testified that the long-term statistical profile is a set of historical averages. (D.I. 592 at 497:1-24; D.I. 593 at 712:13-16) Smaha distinguished a "bit rate" from an "average," and the jury was free to accept that characterization.[12] Plaintiff's motion is denied. The court declines plaintiff's request to award a new trial.

4. ISS's motion for JMOL

ISS moves for JMOL that it does not infringe or induce the infringement of the '615 and '203 patents. The asserted claims require that network monitors (e.g., the ISS Sensors) and an adapted hierarchical monitor (e.g., SiteProtector with Fusion 2.0) be deployed in an "enterprise network." ISS admits that the patents are infringed where ISS Sensors, SiteProtector, and Fusion 2.0 are deployed in an enterprise network and Fusion 2.0's "Attack Pattern Component" ("APC") is enabled and used. (D.I. 570 at 10) Fusion 2.0 also has another functionality, the Impact Analysis Component ("IAC"), which undisputably does not infringe. (D.I. 593 at 702:7-14) The IAC and APC each require separate installation by a customer prior to use. (*Id.* at 702:23-25)

a. Direct infringement by ISS

ISS asserts that plaintiff presented no evidence that ISS itself actually deployed or used the accused products in an infringing manner. (D.I. 570 at 12) Kesidis

---

[12]Because substantial evidence supports the jury's verdict that the ADS does not build short-term statistical profiles, plaintiff's argument that ISS did not refute that ADS "receiv[es] network packets" limitation is of no consequence. (D.I. 569 at 6-7) The court need not address plaintiff's arguments with respect to dependent claims 11, 12 and 13. (*Id.* at 13-14)

admitted at trial that he did not recall "seeing any evidence that ISS itself runs" at least two ISS Sensors with Fusion 2.0. (D.I. 593 at 689:20-690:4) Kesidis described the evidence he saw as "a deployment [by] one of ISS's customers," not ISS. (*Id.* at 645:5-10) In its post-trial papers, plaintiff argues that ISS directly infringes because the evidence shows that: (1) ISS demonstrated Fusion 2.0's APC during training courses; and (2) ISS video presentations, introduced into evidence via computer screenshots, evidence ISS's use of Fusion 2.0's APC.

Plaintiff points to the testimony of Jim Pruss ("Pruss"), ISS's courseware development manager, who designs courses and course materials used to train customers regarding ISS's products.[13] Pruss testified that the APC feature is discussed in ISS's "Advanced SiteProtector" course: "We teach them how to turn that on from a configuration standpoint, and we show them a demonstration. We also describe, at a very high level, types of attack patterns that the product is capable of recognizing." (D.I. 592 at 464:6-13) Plaintiff asserts that "[i]t was reasonable for the jury to infer that to perform [its customer] demonstrations ISS installs SiteProtector and ISS Sensors" because the SiteProtector is a prerequisite to the use of Fusion 2.0, and the APC only analyzes events generated by ISS Sensors. (D.I. 580 at 3) ISS does not contest the latter points. (D.I. 587 at 2-3)[14] Plaintiff also argues that, "during any demonstration of the APC's operation, the APC must actually receive and integrate events, as that is its

---

[13]Testifying by deposition.

[14]The court need not reiterate plaintiff's cited evidence in this regard, but notes that the documentation supports the stated propositions. (*e.g.*, PTX-93 at 535796 (Fusion installation prerequisites include that "SiteProtector must already be installed"); PTX-148)

sole purpose." (D.I. 580 at 3, citing D.I. 570 at 10 ("The APC module combines different reports from the ISS [S]ensors into certain preprogrammed attack types called 'incidents'.")) ISS argues that Pruss testified that ISS instructors use "artificially created traffic" in their demonstrations. (D.I. 592 at 466:22-467:1) ISS also asserts that there is no evidence that the classroom environment satisfied Kesidis' description of an "enterprise network." (D.I. 587 at 2)

Plaintiff also introduced screenshots of Fusion 2.0's APC showing attack patterns generated by Fusion 2.0. (PTX-158; D.I. 592 at 445:15-446:21[15]) Plaintiff asserts that it would be reasonable to assume that ISS deployed SiteProtector and the APC to create the screen images because the screen shots came from the SiteProtector console and show images generated by the APC. (D.I. 580 at 4) Plaintiff also asserts that the jury could have reasonably inferred that ISS deployed ISS Sensors because the APC creates incidents based on receipt of analysis of events generated by deployed ISS Sensors. (*Id.* at 4, citing D.I. 592 at 433:12-16 (generally describing the APC); 436:17-437:4 (the APC cannot analyze events originating from a third party); 445:15-446:21 (PTX-158 shows attack patterns generated by Fusion 2.0)) The above identified documents, however, do not specifically indicate the source of the events. Mr. Paul Griswold, an ISS engineer, testified that incidents can either be based off the

---

[15]Plaintiff also cites PTX-314, a video presentation entitled "RealSecure SiteProtector Overview," and supporting testimony stating that the video shows "automatic correlation," or "analysis without user intervention." (D.I. 580 at 3, citing D.I.594 at 830:6-831:24) Plaintiff does not specifically discuss how this evidence demonstrates infringement. Additionally, ISS points out that the latest "event date" displayed in PTX-314 is November 2002 – prior to the issuance of both the '203 and '615 patents. (D.I. 587 at 3 & ex. A)

attack patterns that are recognized by Fusion 2.0 **or** "[t]hey can be manually created," consistent with Pruss's testimony that artificial traffic may be used for demonstrative purposes. (D.I. 592 at 446:4-8; 466:22-467:1)

Plaintiff points to no testimony affirmatively demonstrating that ISS employed an infringing system during its demonstrations. More specifically, the record is devoid of any indication that, during ISS's classroom demonstrations, an infringing system (multiple ISS Sensors, SiteProtector with Fusion 2.0 and an enabled APC) was actually deployed in an enterprise network. Certainly, Kesidis did not see any evidence of such an occurrence. (D.I. 593 at 689:20-690:4) There is no debate that the APC must receive and integrate events to be functional (and demonstrable), however, there is no indication that, during the customer demonstrations relied upon by plaintiff, the APC necessarily received events from ISS Sensors as compared to an artificial source. On this record, a reasonable jury could not have found direct infringement by ISS by a preponderance of the evidence.

b. Inducement of infringement

Plaintiff avers that it met its burden to show direct infringement at trial in two manners. Plaintiff argues that the system claims (claim 12 of the '203 patent and claims 13, 14 and 16 of the '615 patent) require only that the hierarchical monitors are "adapted to" automatically receive and integrate the reports of suspicious activity, therefore, this limitation is met by merely the **deployment** of ISS Sensors, SiteProtector, and Fusion 2.0 in an enterprise network. That is, plaintiff need not show "evidence of any particular **use** by a customer of the APC." (D.I. 580 at 6) With respect

to the method claims (claim 1 of the '203 patent and claim 1 of the '615 patent), plaintiff asserts that circumstantial evidence such as ISS's training classes and marketing materials demonstrate use of Fusion 2.0 by customers, providing "ample support" for the jury's conclusion that ISS's customers directly infringe. (*Id.* at 8) The court addresses each argument in turn.

i. System claims

As discussed previously, the APC is a component of Fusion 2.0 that has to be installed separately. (D.I. 593 at 702:23-25) Kesidis conceded at trial that a customer who purchases Fusion 2.0 does not necessarily have to install or use the accused APC feature. (*Id.* at 703:1-17 ("I'm assuming that if the APC was purchased with Fusion, I made an argument that it's **likely** that the APC is being used.")) Kesidis did not know for sure whether the APC was actually used by any particular customers. (*Id.* at 703:13-17) Plaintiff generally asserts that, "[b]ased on the fact that Fusion 2.0 must be deployed with SiteProtector and ISS Sensors to be used at all and that ISS instructs its customers to do so, it was reasonable for the jury to conclude that ISS customers do deploy this combination of products as ISS has encouraged them to do." (D.I. 580 at 7-8)

In support, plaintiff cites the following evidence: (1) the APC "[i]nterfaces with SiteProtector to report attack patterns" (PTX-93 at 535790, -793); (2) a "prerequisite" to running Fusion is that "SiteProtector must already be installed" and be directly accessible (*id.* at 535796); (3) "SiteProtector is required" in order to use Fusion (PTX-148 at 5996); (4) "Attack Pattern detection" of Fusion analyzes vulnerability data and

intrusion events collected by SiteProtector (*id.* at 5992); (5) the Fusion module correlates and analyzes events detected by "an intrusion detection agent," or an ISS Sensor (DTX-2501 at 4); (6) Mr. Griswold testified that the APC "will look at multiple [intrusion prevention] events from our sensors," which are received from the "EventCollector," a preprocessor for sensor events that is part of SiteProtector (D.I. 592 at 433:1-16; 434:15-436:21); (7) the APC cannot receive "events that have been generated by third party products" (*id.* at 436:17-21); and (8) Kesidis testified that Fusion 2.0 automatically receives its reports "[f]rom the sensors of the lower level monitors" (D.I. 593 at 654:13-15). (D.I. 580 at 7-8)

ISS does not specifically refute plaintiff's cited evidence that Fusion 2.0 was designed for deployment with SiteProtector and ISS Sensors. (D.I. 587 at 7) ISS instead argues that "a customer's purchase of Fusion 2.0 does not necessarily mean they installed the APC component" (as compared to the IAC component), nor does it mean that Fusion 2.0 with the APC component was installed in an enterprise network where two or more (a plurality of) ISS Sensors were installed. (*Id.*) ISS documentation belies this assertion, however, stating that, "[w]hile it consists of two components [IAC and APC], Fusion is presented as a single homogeneous system to the user." (PTX-93 at 535787)

Nonetheless, plaintiff points to only one example of a customer that used multiple ISS Sensors, SiteProtector and Fusion 2.0 in its network: HealthSouth. (D.I. 580 at 7) Robert Ferrill ("Ferrill"), Director of Information Security for HealthSouth,

testified[16] that HealthSouth uses ISS Sensors, SiteProtector and Fusion 2.0 in its network. (D.I. 592 at 471:17-23) Despite plaintiff's citation to evidence that ISS sold more than $173 million of ISS Sensors to its Fusion 2.0 customers in the United States (D.I. 580 at 8, citing PTX-614), plaintiff points to no testimony, by Ferrill or otherwise, affirmatively indicating that the APC component of Fusion 2.0 was installed by HealthSouth or any other customer.

Fusion 2.0 may have been presented "as a single homogenous system" to HealthSouth,[17] but this is not a substitute for evidence of what any ISS customer(s) actually did. Because it was not disputed that a Fusion 2.0 customer does not necessarily have to install and run the APC feature, plaintiff was required to identify at least one specific instance of infringement by customers, *i.e.*, a customer's use of the APC feature of Fusion 2.0 in an infringing system (multiple ISS Sensors, SiteProtector with Fusion 2.0 and an enabled APC). *See ACCO*, 501 F.3d at 1313. Having failed to do so, the jury's verdict with respect to the system claims must be reversed.[18]

ii. Method claims

With respect to the method claims, and as discussed previously, plaintiff points to evidence that ISS teaches customers how to use the APC feature in ISS's customer

---

[16]By deposition.

[17]This evidence relates to ISS's intent to induce infringement.

[18]Because plaintiff did not introduce evidence sufficient to demonstrate that any ISS customer met the "hierarchical monitors adapted to automatically receive and integrate reports of suspicious activity" limitation, the court need not address the parties' additional arguments regarding claim 16 of the '615 patent, which depends from claim 13.

training course, specifically, "how to configure the product and to recognize that type of event when it appears in the management consult." (D.I. 592 at 464:3-465:5) Additionally, ISS's marketing materials discuss attack pattern recognition. (PTX-148; PTX-157; PTX-314)

Because there is a non-infringing use of Fusion 2.0 (the IAC), under *ACCO*, plaintiff was required to demonstrate that a customer installed the accused APC feature and operated it in an infringing manner. *See ACCO*, 501 F.3d at 1313. There is no affirmative evidence that customers who purchased Fusion 2.0 necessarily ran the infringing combination of software. *Compare Golden Blount*, 438 F.3d at 1361. Nor is there evidence that ISS provided a specific instruction to customers to utilize the APC in this manner. *Compare Moleculon*, 793 F.2d at 1272 (upholding district court finding that plaintiff met its burden of showing infringement under section 271(b) with "circumstantial evidence of extensive puzzle sales, dissemination of an instruction sheet teaching the method of restoring the preselected pattern with each puzzle, and the availability of a solution booklet on how to solve the puzzle"). The jury's verdict was not supported by substantial evidence, therefore, the court grants ISS's motion.

c. Validity of the '338 patent

Claims 1 and 24 of the '338 patent require building "at least one long-term and at least one short-term statistical profile from at least one measure of the network packets," which the court construed to mean "[g]enerating at least two separate data structures . . . where the statistical descriptions are based on at least one measure of the network packets and are generated through the use of statistical analysis[.]" (D.I.

468 at 5) At trial, plaintiff asserted that the JiNao Report disclosed building statistical profiles based on router audit logs, and not network packets, thus failing to satisfy this limitation.

i. The law of anticipation

An anticipation inquiry involves two steps. First, the court must construe the claims of the patent in suit as a matter of law. *See Key Phar. v. Hercon Labs. Corp.*, 161 F.3d 709, 714 (Fed. Cir. 1998). Second, the finder of fact must compare the construed claims against the prior art. *See id.*

Proving a patent invalid by anticipation "requires that the four corners of a single, prior art document describe every element of the claimed invention, either expressly or inherently, such that a person of ordinary skill in the art could practice the invention without undue experimentation." *Advanced Display Sys. Inc. v. Kent State Univ.*, 212 F.3d 1272, 1282 (Fed. Cir. 2000) (citations omitted). The Federal Circuit has stated that "[t]here must be no difference between the claimed invention and the referenced disclosure, as viewed by a person of ordinary skill in the field of the invention." *Scripps Clinic & Research Found. v. Genentech, Inc.,* 927 F.2d 1565, 1576 (Fed. Cir. 1991). The elements of the prior art must be arranged or combined in the same manner as in the claim at issue, but the reference need not satisfy an *ipsissimis verbis* test. *In re Gleave*, 560 F.3d 1331, 1334 (Fed. Cir. Mar. 26, 2009) (citations omitted). "In determining whether a patented invention is [explicitly] anticipated, the claims are read in the context of the patent specification in which they arise and in which the invention is described." *Glaverbel Societe Anonyme v. Northlake Mktg. & Supply, Inc.*, 45 F.3d

1550, 1554 (Fed. Cir. 1995). The prosecution history and the prior art may be consulted "[i]f needed to impart clarity or avoid ambiguity" in ascertaining whether the invention is novel or was previously known in the art. *Id.* (internal citations omitted).

"A claimed invention cannot be anticipated by a prior art reference if the allegedly anticipatory disclosures cited as prior art are not enabled." *Amgen, Inc. v. Hoechst Marion Roussel, Inc.*, 314 F.3d 1313, 1354 (Fed. Cir. 2003). Additionally, the reference must "enable one of ordinary skill in the art to make the invention without undue experimentation." *In re Gleave,* 2009 WL 777398 at *2 (citing *Impax Labs., Inc. v. Aventis Pharms. Inc.*, 545 F.3d 1312, 1314 (Fed. Cir. 2008)). "As long as the reference discloses all of the claim limitations and enables the 'subject matter that falls within the scope of the claims at issue,' the reference anticipates – no 'actual creation or reduction to practice' is required." *In re Gleave,* 2009 WL 777398 at *2 (quoting *Schering Corp. v. Geneva Pharms., Inc.*, 339 F.3d 1373, 1380-81 (Fed. Cir. 2003) and *In re Donohue*, 766 F.2d 531, 533 (Fed. Cir. 1985)).

ii. Discussion

The parties do not dispute that the information being measured in the JiNao system is not "raw" packet data, but is data that comes from, or is derived from, network packets. Kesidis testified that the JiNao system was designed to protect the routing protocol and runs in a router; it "uses statistical profiling to [protect the router] based on audit logs of that process as it's running inside the router." (D.I. 605 at 1884:15-23) Kesidis explained that the JiNao Report discloses that the raw packet data is

transformed into a router-log format.[19] (*Id.* at 1829:18-1830:16; 1888:8-1889:2) The data used by JiNao to perform its statistical analysis is "router logs or audit log information that pertain[s] to information inside the router." (*Id.* at 1884:23-1885:2) Using a demonstrative from a presentation given by the JiNao authors, Kesidis detailed for the jury how a router can receive a message (or network packet) sent directly to it, in its capacity as a "host," and that the network packet is converted to an audit log when it goes through the prevention module.[20] (*Id.* at 1886:2-1887:3) Kesidis supported his opinion with specific references to the JiNao Report. (*Id.* at 1887:17-1894:2)

Valdes also testified that the JiNao Report discussed building profiles based on measures of router table data, as compared to network data. (D.I. 592 at 283:5-8; D.I. 597 at 1523:6-17 ("[W]hat's being analyzed is the [internal router] table, not the [network] packet itself") Valdes was collaborating with the researchers on the JiNao project at the time, as his project and the JiNao project had a common sponsor (DARPA[21]). (D.I. 597 at 1503:14-1504:11; 1516:15) Kesidis testified that DARPA simultaneously funded the EMERALD project focusing on network packets, and DARPA

---

[19]The protocol data unit, or "PDU" format.

[20]The court disagrees with ISS that plaintiff's position on infringement by ADS and validity in view of the JiNao Report is contradictory. (D.I. 587 at 11) ISS emphasizes that, in two-tiered mode, the ADS converts packet data into summary records (or "net flow"). As noted previously, a "packet" was defined by the court as a "group of data bytes which represents a specific information unit with a known beginning and end." (D.I. 468 at 2) There is no indication that summary records of network packets are distinguishable in this regard. Even so, the verdict is not inconsistent with the fact that infringement may be shown by a lower (preponderance of the evidence) standard than that for invalidity (clear and convincing evidence).

[21]The Defense Advanced Research Projects Agency, a division of the Department of Defense.

did not typically duplicate funding in the same research area. (D.I. 605 at 1854:16-24)

There is no dispute that the JiNao Report discussed both audit records and network packets. According to Kesidis, the Report used the two terms distinctly: "audit record" was used in connection with the algorithms that were being implemented; while references to "packets" appear when "high level . . . information and where it may be coming from" was discussed. (*Id.* at 1894:17-1895:10; D.I. 598 at 2029:1-9) Smaha, by contrast, testified for ISS that the authors of the JiNao Report interchangeably used the terms "audit record" and "packets," therefore disclosing a comparison of profiles from at least one measure of network packets. (D.I. 605 at 1727:2-1728:1) ISS argues, alternatively, that because audit records are undeniably derived from network packets, they are "measure[s] of network packets" as required by the '338 patent claims. (D.I. 570 at 25[22])

It was ultimately within the jury's purview to credit the testimony of Kesidis and Valdes over that of Smaha, find router or audit data distinguishable from the "network packets" from which they are derived in the JiNao system, and conclude that clear and convincing evidence did not demonstrate that JiNao Report disclosed building long-term and short-term profiles from at least one measure of network packets.[23] ISS's motion is

---

[22]ISS cites no witness testimony in support for the proposition that an audit record is a "**measure** of the network packets," as compared to a separate entity, as contemplated by the claims. The court notes that the parties did not seek a separate construction of "measure" as used in the claims. (D.I. 174 at 5)

[23]ISS's assertions that the verdict was based on "outrageous assumptions" and would "shock the conscious" if left undisturbed are, themselves, outrageous hyperbole. (D.I. 587 at 13)

denied on this ground,[24] and the court declines to award a new trial.

5. Defendants' motions for JMOL or a new trial regarding validity

a. Anticipation by Live Traffic

The Live Traffic paper discloses all of the limitations in all three patents in suit. (JTX-1 at ¶ 17) The parties dispute, however, whether the Live Traffic paper was publicly available prior to the critical date of November 9, 1997. As discussed *supra*, on August 1, 1997, Porras published the Live Traffic paper to a FTP site maintained by plaintiff, at the following address: ftp.csl.sri.com/pub/emerald/ndss98.ps. (DTX-572) The FTP site could be accessed by the public; it was not password-protected or encrypted. (D.I. 597 at 1365:5-1366:2) The court previously found in favor of defendants on summary judgment, noting that the record demonstrated that Porras provided to colleagues specific links to documents regarding EMERALD on the FTP site (ftp://ftp.csl.sri.com) as early as January 1997, and the FTP site was interchanged as a source of information on an online newsgroup.[25] (D.I. 471 at 13-14) The court was persuaded that a person of ordinary skill in the art of complex computer software technology, upon entering the main FTP site, could readily navigate the two subfolders to access the Live Traffic paper, especially given that the names of the folders ("/pub/")

---

[24]Because the court finds that the jury could have reasonably found that the JiNao Report lacks a limitation required by the independent claims, the court need not address ISS's additional arguments regarding the "hierarchical monitors" limitation of the dependent claims.

[25]The Risks Digest online forum contained two 1994 postings in which papers on plaintiff's FTP site were referenced in the following manners: (1) program and registration form available by "the file /pub/oakland94.txt from ftp.csl.sri.com"'; and (2) more information about the "AAMP5" project available "by ftp from ftp.csl.sri.com/pub/reports/postscript/aamp5.ps.gz. (DTX-1975 at 2-4)

and ("emerald") provided some guidance as to content. (*Id.* at 15) In contrast, the Federal Circuit found that several facts mitigated against a finding of public accessibility: (1) the record contained no indication that members of the public actually accessed and navigated plaintiff's FTP server; (2) Porras thought it necessary to provide the full FTP address to the file to the peer review committee for the paper, as compared to the main address; (3) on past occasions, Porras provided either the full address or filename of papers residing on the FTP servers, indicating that persons of skill in the art required navigational direction; (4) "[n]either the directory structure nor the README[[26]] file in the PUB subdirectory identifies the location of papers or explains the mnemonic structure for files in the EMERALD subdirectory, or any subdirectory for that matter," and the EMERALD subdirectory does not contain a README file; and (5) there was no indication that, "because people had been told that they could find other papers in the past in the /pub/emerald subdirectory, they would – unprompted – look there for an unpublicized paper with a relatively obscure filename." *SRI Intern.*, 511 F.3d at 1198. On remand, the issue of public accessibility of the Live Traffic paper was subsequently tried to the jury, which ultimately found no anticipation by any asserted reference.

Defendants argue post-trial that the trial record refutes any inferences drawn in favor of plaintiff during summary judgment. Porras testified that, generally, people in the field of intrusion detection knew how to download files and documents from FTP

---

[26]Generally, a README file is a text file that contains information about other files in a directory or archive and is commonly distributed with computer software. The file name is chosen so that users are drawn to read it.

sites and often set up their own sites. (D.I. 597 at 1364:15-23) No particular commands were needed to navigate the site. (*Id.* at 1476:2-10) A user could simply click on subdirectories on the ftp.csl.sri.com site or type commands to view files. (*Id.* at 1373:16-24; 1459:14-20)

Porras also confirmed that he circulated FTP addresses in an EMERALD presentation (DTX-60[27]) and in emails to colleagues (DTX-582). (D.I. 597 at 1477:22-1480:16) In one such email, Porras directed the recipients to the "/pub/emerald*.ps" subdirectory of ftp.csl.sri.com, using the asterisk to indicate that several papers about EMERALD could be found in the particular subdirectory. (*Id.*; DTX-582) Defendants introduced a Google search results page displaying postings with links to papers within plaintiff's FTP site. (DTX-1973)

Finally, Porras indicated that regular attendees of the Symposium on Network and Distributed Security Systems, for which the Live Traffic paper was submitted for consideration, would recognize "SNDSS" as the acronym for that conference. (D.I. 597 at 1362:8-24) Brochures for the conference used the similar "NDSS" acronym. (PTX-11) Defendants argue that the Live Traffic paper's "ndss98.ps" filename would have been recognized by persons of skill in the art using plaintiff's FTP site. (D.I. 573 at 39-40)

Notwithstanding the foregoing, substantial evidence supports the jury's verdict

---

[27]The EMERALD presentation provided the following links to "additional information": (1) an "executive summary" at ftp://ftp.csl.sri.com/pub/emerald-position1.ps; (2) an "EMERALD Technical Proposal" at ftp://ftp.csl.sri.com/pub/emerald-12-96.ps; (3) an "API Requirements Statement" at ftp://ftp.csl.sri.com/pub/emerald-api_reqs.ps; and (4) a "Conceptual Review and Planning" document at ftp://ftp.csl.sri.com/pub/emerald-concepts1.ps.

that defendants failed to demonstrate anticipation by clear and convincing evidence. As plaintiff points out, in every instance that Porras directed colleagues to the FTP site, a complete file path was provided.[28] (D.I. 597 at 1499:9-13) As the Federal Circuit previously observed at the summary judgment stage, this is evidence that persons of ordinary skill in the art required navigational direction through the FTP site.

There was also evidence adduced at trial that Porras intended to keep the Live Traffic paper confidential, and was successful in doing so. Porras testified that he emailed the Live Traffic paper to Bishop for consideration for publication, and placed the backup copy on the FTP server out of a concern that the (large) file would be dropped from his email. (*Id.* at 1439:7-1440:6) The Live Traffic paper was posted to the FTP server for seven days, the period of time that the call for papers stated should be allowed for acknowledgment of receipt. (*Id.* at 1438:13-1439:3; PTX-11) An abstract of the Live Traffic paper, along with a statement that the full paper was "in limited distribution" but could be requested by email, was posted on plaintiff's web page the same day it was placed on the FTP server. Despite receiving several email requests, Porras did not provide the full paper until after the critical date for the patents at issue. (PTX-244; PTX-16)

Porras further testified that papers submitted for peer review are considered confidential and are not shared outside of the program chairs. (D.I. 597 at 1440:24-1441:12) Submissions are not discussed outside of the committee and are destroyed

[28]Porras could not recall whether a "read bit," a permissions setting enabling a person to read all of the files in a directory, was set or not set when the Live Traffic paper address was posted; notwithstanding, committee members with the full FTP address for the paper would have been able to access it. (D.I. 597 at 1442:18-1443:14)

after review. (*Id.*) Porras did not intend to publish the paper when the email was sent, only when it was posed on the internet on November 10, 1998. (*Id.* at 1440:19-21; 1457:17-22)

The jury was instructed that, "[i]n determining whether a document is a 'printed publication,' factors such as the intent to make public, activity in disseminating information, production of a certain number of copies, and production by a method allowing reproduction of a large number of copies may be considered," and that "[c]onfidential documents are not 'printed publications.'" (D.I. 550 at 33) Porras's intent to keep the Live Traffic paper confidential until November 10, 1998 was a proper consideration for the jury. In view of the foregoing, as well as the lack of evidence regarding any index or classification system existing on the FTP site or of any particular incentive on behalf of the public to browse the FTP site for (unpublicized) papers, the court finds that substantial evidence supports the verdict of no anticipation by the Live Traffic paper.

b. Anticipation by RealSecure

Defendants also assert that clear and convincing evidence was presented with respect to anticipation of the '203 and '615 patent claims by RealSecure. At issue in this regard is whether RealSecure performed "integration" as required by the claims. The court construed the limitation "automatically receiving and integrating reports of suspicious activity" as follows: "[w]ithout user intervention, receiving reports of suspicious activity and combining those reports into a different end product; *i.e.*, something more than simply collecting and reiterating data." (D.I. 550 at 20)

Defendants' primary argument is that plaintiff admitted at trial that RealSecure performed "correlating" of intrusion reports, as required by dependent claim 14 of the '615 patent, and, therefore, RealSecure necessarily performed the "integrating" limitation of the independent claim from which claim 14 depends. "Correlating" was defined by the court to mean "[c]ombining the reports to reflect underlying commonalities." (*Id.*)

In support for their argument, defendants point to Kesidis' testimony on cross examination, as compared to any of the admitted exhibits regarding RealSecure.[29] (D.I. 573 at 29; D.I. 588 at 16) Kesidis testified (based upon his review of documents) that RealSecure "sorted" reports, though he may have used the word "grouped" in the context of summarizing events. (D.I. 605 at 1937:7-1938:16) Kesidis stated that "grouping" is "combining" in the "plain meaning of the word." (*Id.*) Kesidis also testified that this "combination or sorting . . . is a trivial one . . . it certainly isn't meaningful necessarily for intrusion detection." (*Id.* at 1942:5-8) In his opinion, this was no more than "merely collecting and reiterating the data," and more was required by the claims. (*Id.* at 1942:9-17) This testimony was reasonably consistent with his direct examination, wherein he explained that the RealSecure console only collects, reiterates, and sorts the events – "a human being is required to plow through this stuff and make intrusion detection decisions." (*Id.* at 1859:5-18 (noting a "big difference"

[29](DTX-1704 (RealSecure 1.1 user guide); DTX-1705 (RealSecure 1.0 user guide); DTX-1706 (ISS website entitled "More About RealSecure"); DTX-2110 ("Frequently Asked Questions about RealSecure"); DTX-2112 (ISS website describing RealSecure); DTX-2542 (RealSecure 1.0 for Windows NT user guide)) The RealSecure user guide, for example, never describes RealSecure as either "correlating" or "integrating" events. (DTX-2542 at Figs. 24, 25, 26)

between this and "correlating the events meaningfully in the context of intrusion detection"); 1823:11-18; 1863:16-19 (a person of ordinary skill in the art in 1998 would not have considered RealSecure to be doing automatic correlation or integration); D.I. 598 at 2015:14-2016:15 (RealSecure "simply sorted" events into directories)) In Kesidis's opinion, if RealSecure did do automatic integration, there would have been no need to design Fusion 2.0 (with correlation capabilities) years later. (D.I. 605 at 1825:20-24)

The jury also heard testimony from Holly Stewart, ISS product manager and technical writer for the RealSecure Server Sensor,[30] that "pattern recognition was a new feature of Fusion 2.0. . . before Fusion 2.0, the customer would have to manually create an incident in SiteProtector if they wanted to associate a group of events and call that out distinctly at the incident." (D.I. 592 at 458:21-459:4) The jury was aware that the Patent Examiner considered RealSecure prior to issuing the '615 patent. (D.I. 605 at 1825:8-12; 1862:13-17)

Defendants emphasize that RealSecure's Activity Tree combined reports of suspicious network activity into a "differently organized" end product. (D.I. 573 at 32) Joe Kleinwaechter, ISS operations manager, testified that the information displayed by the Activity Tree was not simply a reiteration of events; the total count of events ("(X)") is "valuable information" to the user about the significance of events. (D.I. 594 at 802:9-12; 807:10-25) Kesidis agreed that the Activity Tree sorts the events

[30]Testifying by deposition.

"a different way"[31] (D.I. 598 at 2015:23) and combines identical events, insofar as those events are counted. (D.I. 605 at 1936:21-1937:10) Kesidis made clear, however, that he did not equate "counting up identical events for the purpose[ ] of displaying them" with "automatic integration" of reports as required by the patents, because human analysis is still required to determine a significant security threat and because the console still stores events individually after they are tallied. (*Id.* at 1823:2-15)

Ultimately, the jury was presented with a credibility determination and was free to accept Kesidis's view of the prior art. In view of the foregoing, the court finds that substantial evidence supports the jury's verdict that RealSecure did not anticipate the asserted claims.

c. Anticipation by the DIDS 1991 paper

At issue between the parties is whether the DIDS 1991 paper disclosed "deploying a plurality of network monitors in an enterprise network." Defendants rely on only one specific disclosure of the DIDS 1991 paper in this respect: that "a single LAN monitor for each LAN segment of the monitored network." (DTX-21 at 168) Defendants argue that, on cross examination, Kesidis admitted that the DIDS 1991 paper discloses that, "[i]f you have two LAN segments, you need two LAN monitors." (D.I. 605 at 1917:4-5) Kesidis testified, however, that there is no teaching regarding how a DIDS system with multiple LAN monitors would be created. (*Id.* at 1828:11-16; 1917:8-9 ("It doesn't teach how to hierarchically integrate [multiple LAN segments] into a DIDS director [the hierarchical monitor].")) Defendants' expert, L. Todd Heberlein

[31]Defendants cite no testimony by Kesidis that events are combined into a "different end product" as per the court's claim construction. (D.I. 573 at 33)

("Heberlein"), testified for defendants that the DIDS 1991 paper describes and explains that the DIDS director integrates and correlates information from multiple sources. (D.I. 594 at 1016:25-1017:14)

Defendants point to no actual disclosure in the DIDS 1991 paper of the use of multiple LAN monitors – only a statement that more than one LAN monitor would be required in the event more than one LAN segment was employed. That Smaha testified that a DIDS system was built with multiple network monitors does not alter this fact. (D.I. 588 at 27, citing D.I. 597 at 1584:20-1585:19) The court does not disturb the jury's verdict of no anticipation on this record. Because there is no indication that the DIDS 1991 paper disclosed all of the claimed limitations, the court need not reach the parties' arguments regarding enablement.

d. EMERALD 1997

i. Anticipation and the effect of the prior rulings

In its opening post-trial brief, defendants briefly argued that EMERALD 1997 anticipates the claims of the '615 patent, and the jury's verdict of no anticipation was not supported by the evidence in this regard. (D.I. 573 at 25-27) This argument was addressed cursorily in a footnote in plaintiff's opposition papers (D.I. 578 at 48, n.21), and defendants did not discuss anticipation by EMERALD 1997 in their reply (D.I. 588 at 1). EMERALD 1997 is listed as a reference on the face of the '615 patent. Defendants' burden to demonstrate anticipation of a reference before the PTO was a heightened one. *See Hewlett-Packard Co. v. Bausch & Lomb Inc.*, 909 F.2d 1464, 1467 (Fed. Cir. 1990). The court notes that Kesidis testified that EMERALD 1997 lacks

a disclosure of the claimed network traffic data categories. (D.I. 605 at 1839:13-1845:25) Further, "[t]here's no discussion as to specifically how to do detection," and the knowledge of the existence of an attack and how it works does not point persons of ordinary skill in the art to a particular method of detecting that attack. (*Id.* at 1846:1-10; 1847:25-1848:4) The court is not inclined to reverse the verdict of the jury on this record.

ii. The law of obviousness

"A patent may not be obtained . . . if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art." 35 U.S.C. § 103(a). Obviousness is a question of law, which depends on several underlying factual inquiries.

> Under § 103, the scope and content of the prior art are to be determined; differences between the prior art and the claims at issue are to be ascertained; and the level of ordinary skill in the pertinent art resolved. Against this background the obviousness or nonobviousness of the subject matter is determined. Such secondary considerations as commercial success, long felt but unsolved needs, failure of others, etc., might be utilized to give light to the circumstances surrounding the origin of the subject matter sought to be patented.

KSR Int'l Co. v. Teleflex Inc., 550 U.S. 398, 405 (2007) (quoting *Graham v. John Deere Co.*, 383 U.S. 1, 17-18 (1966)). "Because patents are presumed to be valid, *see* 35 U.S.C. § 282, an alleged infringer seeking to invalidate a patent on obviousness grounds must establish its obviousness by facts supported by clear and convincing evidence." *Kao Corp. v. Unilever U.S., Inc.*, 441 F.3d 963, 968 (Fed. Cir. 2006) (citation omitted).

"[A] patent composed of several elements is not proved obvious merely by demonstrating that each of its elements was, independently, known in the prior art." *KSR*, 550 U.S. at 418. Likewise, a defendant asserting obviousness in view of a combination of references has the burden to show, by clear and convincing evidence, that a person of ordinary skill in the relevant field had a reason to combine the elements in the manner claimed. *Id.* The Supreme Court has emphasized the need for courts to value "common sense" over "rigid preventative rules" in determining whether a motivation to combine existed. *Id.* at 419-20. "[A]ny need or problem known in the field of endeavor at the time of invention and addressed by the patent can provide a reason for combining the elements in the manner claimed." *Id.* at 420.

In addition to showing that a person of ordinary skill in the art would have had reason to attempt to make the composition or device, or carry out the claimed process, a defendant must also demonstrate, by clear and convincing evidence, that "such a person would have had a reasonable expectation of success in doing so." *PharmaStem Therapeutics, Inc. v. ViaCell, Inc.*, 491 F.3d 1342, 1360 (Fed. Cir. 2007).

iii. EMERALD 1997 alone

Defendants' obviousness theory with respect to EMERALD 1997 is as follows: (1) the prior rulings in this case establish that "all but one small portion of the '203 and '615 patent claims – the element regarding the claimed categories of network traffic data[32] – were disclosed and enabled by EMERALD 1997"; (2) the claimed categories

---

[32]Claim 1 of the '615 patent requires detecting suspicious network activity based on analysis of network traffic data "selected from one or more of the following categories: {network packet data transfer commands, network packet data transfer errors, network packet data volume, network connection requests, network connection

of network traffic data were not novel, and were well known in the art; and (3) "[o]bviously a person skilled in the art . . . would have been aware of one or more of the 'common' categories used to monitor network traffic and would have had a reasonable expectation of success in using these categories for network monitoring." (D.I. 573 at 6, 9-10) In support, defendants cite testimony that persons of ordinary skill in the art had been measuring certain named types of network data for some time. Most notable in this regard is Kesidis' acknowledgment that network packet data volume was a "fairly common" type of network traffic data to monitor. (*Id.* at 10, citing D.I. 593 at 696:1-22) Additionally, Porras acknowledged that "people in the field of intrusion detection already knew how to detect suspicious network activity by analyzing at least one of your network traffic data categories, network connection requests." (D.I. 588, citing D.I. 595 at 1360:1-12)

> In appropriate circumstances, a single prior art reference can render a claim obvious. However, there must be a showing of a suggestion or motivation to modify the teachings of that reference to the claimed invention in order to support the obviousness conclusion. This suggestion or motivation may be derived from the prior art reference itself, . . . , from the knowledge of one of ordinary skill in the art, or from the nature of the problem to be solved.

SIBIA Neurosciences, Inc. v. Cadus Pharm. Corp., 225 F.3d 1349, 1356 (Fed. Cir. 2000) (internal citations omitted). Defendants point to no specific testimony regarding a suggestion or motivation to modify the teachings of EMERALD 1997 to analyze any of

---

denials, error codes included in a network packet, network connection acknowledgements, and network packets indicative of well-known network-service protocols}." Claim 1 of the '203 patent is equivalent except that network connection acknowledgements or network packets indicative of well-known network-service protocols are not included among the categories of network traffic data.

the claimed categories of network traffic data.[33] (D.I. 573 at 10, 18; D.I. 588 at 3) Defendants instead assert that one or more cited categories would have been "obvious to try," based upon the "common sense" of persons of ordinary skill in the intrusion detection field. (D.I. 588 at 3-4, 18)

In sum, substantial evidence supports the conclusion that defendants did not make out a prima facie case of obviousness, insofar as they did not adduce evidence of a specific motivation to modify EMERALD 1997 to yield the embodiment of the claims, or a reasonable expectation of success in doing so. The jury did not err in finding that defendants failed to meet their high burden of proof on obviousness.[34] Moreover, the verdict is supported by substantial evidence adduced by plaintiff at trial. For example, Porras testified that, in 1997, people in the field "had just broad ideas of the kinds of data that we would be interested in"; he did not know what kind of network traffic he would end up focusing on, how to measure that data, what specific statistical measures would be used, or how data would be reported from lower levels to higher levels and correlated. (D.I. 592 at 356:10-20; 361:14-25; 366:1-20) Porras characterized EMERALD 1997 as an "explanation of what [he] was envisioning." (*Id.* at 361:16-17)

---

[33]Kesidis, testifying as to infringement, noted that monitoring certain types of network data (*e.g.*, packet data volume) would be useful in monitoring for particular attack patterns (*e.g.*, a "denial of service attack"). (D.I. 573 at 17, citing D.I. 593 at 606:2-608:14; 649:18-650:12; 698:4-699:15 (cross-examination)) This testimony by plaintiff's expert, however, did not address obviousness nor the motivation to modify the teachings of EMERALD 1997.

[34]As noted previously, EMERALD 1997 was before the PTO during prosecution of the '615 patent, rendering a finding of obviousness with respect to that patent "especially difficult." *Hewlett-Packard*, 909 F.2d at 1467. EMERALD 1997 was also before the PTO during prosecution of the '338 patent.

The paper listed "categories of data that [Porras was] going to consider as candidates." (*Id.* at 366:21-24) A peer reviewer characterized EMERALD 1997 as a "starting point for a fruitful thread of research" and a "research proposal." (DTX-536) Porras explained that, after drafting EMERALD 1997, it took nine months of work to develop the "architectural design" of the system, perform "the analysis of the data itself," and iron out "all the other problems that would occur in trying to develop out a scalable system that could scale up to very large networks."[35] (D.I. 592 at 362:4-22) After nine months of efforts, Porras and Valdes narrowed the universe of data that could be extracted from network data to the "small subset" of measures claimed in the patents. (*Id.* at 376:8-378:12)

Kesidis testified that EMERALD 1997 lacks "the selection of network packet data, which is the basis of intrusion detection, as well as the features that are extracted from that kind of data," and testified that these features were not suggested in the paper.[36] (D.I. 605 at 1820:6-13) Additionally, a person of ordinary skill in the art (having knowledge of certain types of network attacks) viewing EMERALD 1997 would not have arrived at the claimed inventions, as "[i]t's clear from the paper itself that there are different ways of detecting intrusions." (*Id.* at 1820:24-25) EMERALD 1997 discussed "a well-known problem of detecting intrusions in an enterprise network. There [were] lots of smart people working on it. And if [it was] just a matter of

---

[35]After this nine months, Porras co-authored the Live Traffic paper, which undisputably discloses all aspects of the claimed inventions. (D.I. 592 at 362:18-22)

[36]Kesidis specifically disagreed with each of Heberlein's examples of purported disclosures corresponding to the claimed network data categories in EMERALD 1997: SNMP; "network datagrams"; and "application logs." (D.I. 605 at 1839:13-1845:25)

assembling stuff together, it would have been done already by one of them," in contrast to the months of work invested by Porras and Valdes.[37] (*Id.* at 1821:30-1822:6; *see also* DTX-2204 at 28 ("The challenge presented by these products is to determine the appropriate data to be collected. Collecting all possible data would constrain these products due to the limitations of storage space.")) Had defendants established a prima facie case, the foregoing evidence would have been relevant rebuttal evidence.[38] The

---

[37]In connection with its brief anticipation argument, defendants suggested that the jury finding of no anticipation is inconsistent with plaintiff's prior arguments (and the Federal Circuit's finding that) EMERALD 1997 was sufficiently enabled so as to anticipate the related '212 patent. (D.I. 573 at 4, 6, 27) The prior finding that EMERALD 1997 is enabled does not preclude the jury's finding that defendants did not demonstrate invalidity of the '203 and '615 patents by clear and convincing evidence. *See In Re Gleave*, 560 F.3d 1331, 1335 (Fed. Cir. 2009) ("The only way one can show that a reference enables [a] method is to show that a person of ordinary skill would know how to use – in other words, to practice or carry out – the method in light of the reference. This does not mean, however, that the prior art reference must demonstrate the invention's **utility**.") (emphasis in original); *In re Hafner*, 410 F.2d 1403, 1405 (C.C.P.A. 1969) ("[Section] 112 provides that the specification must enable one skilled in the art to 'use' the invention whereas § 102 makes no such requirement as to an anticipatory disclosure.") (cited by *In re Gleave*). The enablement hurdle for a prior art reference is lower than the clear and convincing burden of proof for demonstrating obviousness, or that an invention "is more than the predictable use of prior art elements according to their established functions." *KSR*, 550 U.S. at 417. EMERALD 1997, enabled for § 102 purposes, could have nevertheless failed to provide an obvious solution for a known problem in the art.

[38]The court notes that plaintiff proffered evidence on secondary considerations (objective indicia) of non-obviousness. The existence of secondary considerations is a question of fact. *See Heidelberg Harris, Inc. v. Mitsubishi Heavy Indus., Ltd.*, Civ. Nos. 99-1100, 99-1101, 99-1102, 2000 WL 1375270, *11 (Fed. Cir. Sept. 18, 2000). However, "[a] nexus between the merits of the claimed invention and evidence of secondary considerations is required in order for the evidence to be given substantial weight in an obviousness decision." *Muniauction, Inc. v. Thomson Corp.*, 532 F.3d 1318, 1327 (Fed. Cir. 2008). Plaintiff points to no testimony (by Kesidis or otherwise) specifically addressing the nexus requirement in the context of the objective indicia of non-obviousness, more specifically, the commercial success of the invention. Plaintiff cites evidence that defendants promoted their products as performing correlation, an aspect of the claims. (*E.g.*, PTX-157 (Fusion product brochure touts two added

jury's verdict is affirmed.

iv. EMERALD 1997 in view of Intrusive Activity 1991

At trial, Heberlein testified that Intrusive Activity 1991 disclosed a method of detecting suspicious activity using two of the claimed categories of network traffic data: network packet data volume, and network connection requests. (D.I. 595 at 1094:23-25; 1100:20-1101:9; 1095:3-1098:4) According to defendants, EMERALD 1997 provides an explicit motivation to combine its teachings with Intrusive Activity 1991, an internally cited reference. (D.I. 573 at 12)

A discussion of "Related Work" is provided prior to the "conclusions" section of EMERALD 1997. Under the subtitle "Related Intrusion Detection Research," EMERALD 1997 states:

> Various other efforts have considered one of the two types of analysis – signature-based (*e.g.*, Porras [18] has used a state-transition approach; the U.C. Davis and Trident DIDS [4] addresses abstracted analysis for networking, but not

---

"automated and advanced correlation techniques"); PTX-162 (ISS presentation highlighting that with Fusion, customers can buy more sensors and protect more assets without manual analysis); PTX-30 (plaintiff's strategy was to use correlation technologies as the "building blocks" for enterprise customers); PTX-60 at SYM_P_37109 ("Correlation Analysis Framework" was a main component of ManHunt)) (cited at D.I. 578 at 59)) This evidence would be indicative of the commercial success of an invention relating to correlation, not a combination of correlation and other processes and/or features. Plaintiff effectively argues that the correlation feature is coextensive with (and cannot be separated from) the rest of the claims; again, no specific testimony to this effect is provided. (D.I. 578 at 57-60) Kesidis did not specifically testify, as plaintiff asserts, "that the selective monitoring and integration of reams of data constituted the essence of the patented invention," nor does plaintiff cite any specific evidence linking these two features to the commercial success of defendant's products. (*Id.*, citing D.I. 593 at 595:1-596:18) In fact, Kesidis admitted on cross-examination that he did no analysis to determine the impact that the non-infringing component of Fusion 2.0 or of ISS's Sensors had on the sales of those products. (D.I. 598 at 2009:19-25) Because defendants did not establish a prima facie case of obviousness, the foregoing deficiency was not fatal to plaintiff's case.

> scalability; the Network Security Monitor [7] [[Intrusive Activity 1991]] seeks to analyze packet data rather than conventional audit trails; Purdue [5] seeks to use adaptive-agent technology) or profile-based. More recent work in UC Davis' GrIDS effort [24] employs activity graphs of network operations to search for traffic patterns that may indicate network-wide coordinated attacks.

(DTX-356 at 364) Heberlein testified that this disclosure communicated to persons of ordinary skill in the art "that there's a system that already analyzes network packets, called network security monitor. If you want more information, follow the link number seven." (D.I. 595 at 1092:1-4; *see also id.* at 1092:25-1093:6 ("It has more details that you can use to analyze network traffic.")) Heberlein further testified that one of ordinary skill in the art would have combined the references. (*Id.* at 1093:7-9) With respect to a motivation to combine, Heberlein merely cited the fact that Intrusive Activity 1991 was cited as an additional source of information regarding analyzing network traffic. (*Id.* at 1101:20-1102:6) Defendants also argue that, by citing Intrusive Activity 1991, Porras was "inviting the reader to go and read [that paper] if they were interested in further information on monitoring network packets." (D.I. 573 at 13, citing D.I. 597 at 1353:11-15)

In response, plaintiff stresses that Intrusive Activity 1991 described a system operating on a LAN, not an enterprise network. (D.I. 578 at 50, citing D.I. 595 at 1097:21-1098:12) Kesidis testified that Intrusive Activity 1991 was one of a "laundry list of references" mentioned in EMERALD 1997, and that the two papers "teach away from each other" because they addressed different problems. (D.I. 605 at 1822:19-1823:2) More specifically, "EMERALD [1997] is trying to deal with a very large communication network, very complex, distributed network, and Intrusive Activity [1991], in my opinion,

would have scalability problems. But in a more fundamental way, I don't believe Intrusive Activity [1991] specifically discloses a method of doing detection." (*Id.* at 1850:18-1851:8; 1852:7-10) Additionally,

> [t]he EMERALD [1997] paper is talking about a profiler engine being dedicated to a specific target event stream at the elementary level. . . . The idea here, it was understood in 1997 that you couldn't look at everything. You couldn't look at all the features of all the packets. You had to be selective. And so they were very concerned that the sensors, the monitors of any kind, the lower level or the hierarchical monitors, were scalable to the situation.

(*Id.* at 1851:18-1852:6) Intrusive Activity 1991 "could not scale and function well in this context." (*Id.* at 1852:9-10)

In the case at bar, the jury could have reasonably credited the testimony of Kesidis over Heberlein and concluded that, despite EMERALD 1997's reference to Intrusive Activity 1991, persons of ordinary skill in the art would not have a motivation to combine the two in the context of an enterprise network as claimed. Further, defendants point to no particular testimony relating to the reasonable expectation of success in its post-trial papers. Kesidis's testimony cast doubt on the expectation that making the claimed combination of EMERALD 1997 and Intrusive Activity 1991 would function well in a large network, and could have been properly credited by the jury. In short, substantial evidence supports the jury's verdict that defendants did not meet their high burden to prove obviousness at trial.

6. Defendants' motions for JMOL or a new trial based on evidentiary issues and procedural matters

Defendants argue that a new trial should be granted due to the court's error in its treatment of claim construction and several evidentiary issues. Defendants first argue

that the verdict was so against the clear weight of the evidence that "manifest injustice" will result absent a new trial. (D.I. 573 at 47) For the reasons discussed above, the court does not find the verdicts of validity to be against the weight of the evidence.

Defendants also argue that the court's refusal to instruct the jury "that the '212 patent had been held to be invalid and therefore most of the limitations of the '203 and '615 patents were disclosed and enabled by the EMERALD 1997 reference" was prejudicial error. (*Id.* at 53) Defendants emphasize that Kesidis originally testified that EMERALD 1997 did not disclose monitoring network traffic data or how to perform intrusion detection. (D.I. 605 at 1838:17-20; 1846:1-7; 1853:25-1854:5; 1900:7-11; 1904:12-17) Defendants acknowledge that Kesidis withdrew these opinions on cross-examination, but assert that "the damage was already done." (*Id.* at 1920:11-1921:5) The court disagrees that a limiting instruction was required. It was within counsel's purview, not the court's, to emphasize this change of opinion to the jury. The jury was fully capable of judging Kesidis's credibility.

The next ground for defendants' motion is the court's failure to admit any evidence relating to the co-pending reexaminations of the patents in suit. Absent unusual circumstances, none of which were presented here, non-final[39] decisions made during reexamination are not binding, moreover, they are more prejudicial (considering the overwhelming possibility of jury confusion) than probative of validity. *See Callaway Golf Co. v. Acushnet Co.*, — F.3d —, 2009 WL 2481986, *9 (Fed. Cir. Aug. 14, 2009) (stating that non-final reexamination determinations "of little relevance to the jury's

[39]Decisions not vetted by the Federal Circuit.

independent deliberations on the factual issues underlying the question of obviousness" in contrast to the risk of jury confusion); *Amphenol T & M Antennas, Inc. v. Centurion Intern., Inc.*, 69 U.S.P.Q.2d 1798, 1800 (N.D. Ill. 2002) ("[T]elling the jury that the patent has been called into question by the Patent Office may significantly influence the jury's application of the presumption of validity and significantly prejudice ATM. The prejudicial potential of this evidence far outweighs any probative value it may have."). Defendants' suggestion that "an adjustment to the standard jury instructions regarding the burden of proof" on invalidity was warranted in view of the copending reexamination is, at best, untenable. The court declines to rewrite reams of patent litigation jurisprudence and be the first to ignore a patent's presumption of validity and apply the lower preponderance of the evidence standard to invalidity claims.

Defendants also assert that the court incorrectly amended its construction during trial, to its surprise and detriment. In October 2006, the court construed "hierarchical monitor/hierarchical higher network monitor" as "a network monitor that receives data from at least one network monitor that is at a lower level in the analysis hierarchy." (D.I. 468) "[A] plurality of network monitors" was defined as "two or more network monitors." (*Id.*) The asserted claims required a plurality of network monitors detecting suspicious network activity based on analysis of network traffic data, and one or more hierarchical monitors; put most simply, at least two higher-level monitors and one lower-level monitor. During trial, Heberlein testified that "we've got dueling claim constructions here, but using the court's claim construction, a hierarchical monitor is also considered a network monitor and the lower level is called a network monitor. So they're all called network monitors. All the monitors are called network monitors." (D.I. 596 at 1231:1-

10) Heberlein clearly suggested to the jury that a system with a single higher level monitor and lower level monitor could encompass a "plurality of network monitors" as required by the claims. (*Id.*) As a result, prior to closing arguments, the court issued the following instruction:

> Symantec has presented evidence on the hierarchical monitoring claims through its expert, Mr. Heberlein, to suggest that the claims only require a minimum of two monitors, one serving as a network monitor and one serving as a hierarchical network monitor. During Mr. Heberlein's testimony, I, the court, clarified its claim construction in this regard: Thus, requiring that the enterprise network have a minimum of three monitors, two serving as network monitors and one serving as a hierarchical monitor. Therefore, to the extent that Mr. Heberlein testified contrary to the court's claim construction, you should disregard this testimony.

(D.I. 598 at 2091:15-2092:6)

The court discerns no error or prejudice in its action. The court clarified, but did not replace or revise, its prior claim construction. Defendants' claim of unfair surprise and prejudice, therefore, is unfounded. Heberlein's testimony that two "competing" claim constructions were to be evaluated was inappropriate at best, abusive at worst. Accordingly, the court properly performed its gatekeeping function. Defendants' motion is denied on this ground.

V. CONCLUSION

For the foregoing reasons, the court: (1) denies plaintiff's motion for post-trial relief regarding ISS's infringement of the '338 patent (D.I. 564); (2) grants ISS's motion for JMOL with respect to non-infringement of the '203 and '615 patents, and denies the motion (D.I. 565) in all other respects; (3) grants Symantec's motion for JMOL with respect to non-infringement by the SGS and Manager Products (D.I. 567); (4) and denies Symantec's motion for a new trial or to amend the judgment (D.I. 566). As

Symantec did not contest the jury verdicts of direct infringement and inducement of infringement by its ManHunt products, the court enters judgment for plaintiff and against Symantec. The court also enters judgment for ISS with respect to its counterclaims of noninfringement of the '338, '203 and '615 patents (D.I. 38 at ¶ 23; D.I. 40 at ¶ 37). An appropriate order shall issue.